Carrillo-Nunez, H., Wang, C., Asenov, A., Young, R. and Georgiev, V. (2019) Simulation of Si Nanowire Quantum-Dot Devices for Authentication. In: 2019 Joint International EUROSOI Workshop and International Conference on Ultimate Integration on Silicon (EUROSOI-ULIS), Grenoble, France, 01-03 Apr 2019, ISBN 9781728116587.

There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

http://eprints.gla.ac.uk/218301/

Deposited on: 15 June 2020

Enlighten – Research publications by members of the University of Glasgow
http://eprints.gla.ac.uk

Simulation of Si nanowire quantum-dot devices for authentication

Hamilton Carrillo-Nunez[1], Chen Wang[2], Asen Asenov[1], Robert Young[2], Vihar Georgiev[1]
[1]Device Modelling Group, School of Engineering, University of Glasgow, Glasgow, G12 8QQ, UK
[2]Young-Quantum Group, Department of Physics, Lancaster University, Lancaster, LA1 4YB, UK
e-mail: vihar.georgiev@glasgow.ac.uk

***Abstract*—This paper shows quantum mechanical simulations of quantum-dots (QDs) embedded within Si nanowires. To capture the effect of statistical sources of variability, we simulated 60 wires with differing numbers and positions of dopants, not only in the quantum dot but also at the source and the drain regions also. Our work shows that the specific number of dopants and their positions give rise to unique current-voltage characteristics, providing unique signatures for use as the basis of physical unclonable functions (PUFs). Adoption of hardware security devices for authentication is on the rise; the technology proposed here delivers a practical means to extract fingerprints from quantum confined systems that could provide robust security to silicon electronics.**

Keywords: quantum mechanical simulations, Physical Unclonable Function, resonant tunneling quantum-dots

I. Introduction

Physical unclonable functions (PUF) are considered as one of the most promising methods for hardware authentication [1-4]. PUFs are typically compact devices providing a response when challenged that is linked to uncontrollable stochastic processes and physics variability that occur during hardware manufacturing [5], [6]. As a result, it is practically impossible to produce two identical devices, which is highly desirable for applications in cybersecurity. For example, an important source of statistical variability in semiconductor nano-electronics, which has a huge impact on the electrical characteristics of each device, is the random dopant distribution (RDD) within the structure. The stochastic nature of the RDD profile for each device leads to a unique electrical output for each device. Indeed, this is the main idea and strength behind PUFs based on quantum dots that can be fabricated using standard CMOS technology and processes. In addition, as the dimensions of the modern transistors range from a few to tens of nanometers, there is a unique opportunity to use quantum mechanical effects, such as confinement and tunneling, as another layer of security based on quantum effects.

One possible device structure that can be fabricated using the standard CMOS process and that can be implemented in current electrical circuits is a quantum-dot-in-wire device, which is considered in this work. the dot device relies on tunneling of electrons through a barrier and for this reason it can be considered a device that provides a quantum fingerprint.

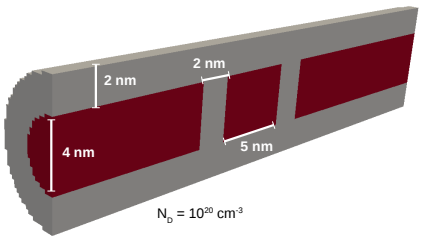

Figure 1. Sketch of the Si nanowire QD along the transport direction considered in this work. All Si (red) regions are highly doped with $N_D = 10^{20}$ cm^{-3}. The oxide (gray) regions are made of SiO_2.

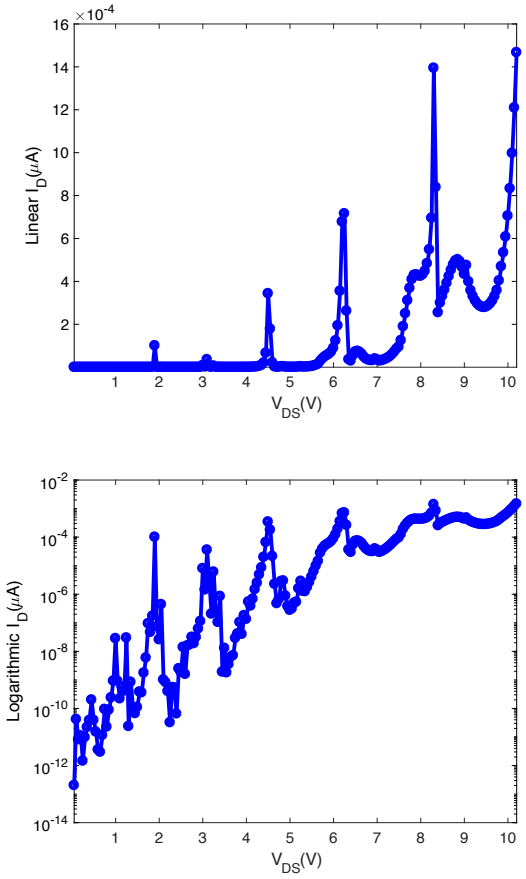

Figure 2. Top (linear scale) and bottom (log scale) of the I–V_{DS} characteristics of a uniform (smooth) Si dot-in-wire device without any sources of statistical variability. Peaks in the spectrum result from resonant tunnelling through the device.

Authorized licensed use limited to: University of Glasgow. Downloaded on June 11,2020 at 10:48:32 UTC from IEEE Xplore. Restrictions apply.

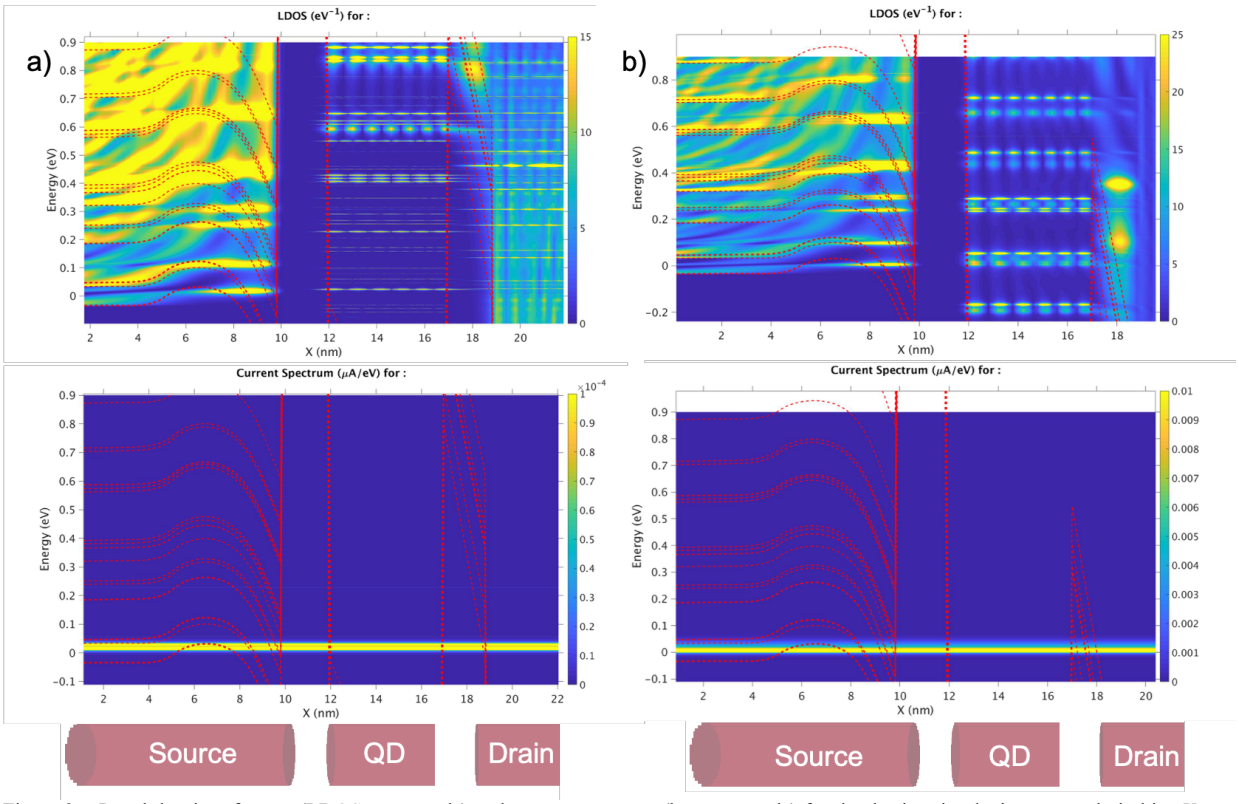

Figure 3. Local density of states (LDOS, top panels) and current spectrum (bottom panels) for the dot-in-wire device at two drain bias V_{DS} = 4.5 V (a) and at V_{DS} = 6.1 V (b). The red lines are the subband profiles and the color profiles represent the device's LDOS and current spectra for the top and bottom panels respeectively, in arbitrary units.

II. Methodology and Results

Simulations of dot-in-wire devices in this work were carried out by employing the Non-Equilibrium Green's function (NEGF) approach, implemented in the device simulation framework, NESS [7]. Quantum transport is solved within the effective mass approximation with mode-space representation. This technique is coupled self-consistently to the Poisson equation numerical solver. The total carrier density determines the new potentials which is then input into the NEGF solver for a new current and charge distribution within the active region of the device. The self-consistent loop is repeated until the specific criterion of convergence is reached.

Fig. 1 shows the geometry of the dot-in-wire considered in this work. It is built from two semi-infinite Si nanowire (source/drain) leads and a Si quantum-dot isolated by two oxide layers, which act as tunneling barriers (TBs). All Si regions high doped n-type with the concentrations of the donors, $N_D = 10^{20}$ cm^{-3}. The Si nanowire channel is 4 nm in diameter and the quantum dot is 5 nm long in the transport direction. The TBs are symmetric with a length of 2 nm.

Fig. 2 shows the current-voltage characteristics (I-V_{DS}) for the uniform device, which is a device without any sources of variability. From this figure it is clear that the I-V_{DS} curves shows significant oscillation with a large number of peaks. Each peak in the current corresponds to resonant tunneling of electrons through the SiO_2 TB from the sources to the QD. The source-to-drain tunneling occurs when a QD energy level is aligned with the electron injection energy from the source or the quasi-localized state generated at the TB interface. The latter can be seen in Fig. 3 at the bottom. There, the local-density-of-states (LDOS) and the current spectrum are shown for the uniform device at two different drain biases. The red lines follow the subband energy profiles.

Fig. 3 a) shows the LDOS within source and QD regions. One can see the discreteness of the LDOS in the QD, due to quantum confinement from width of the dot defined by TBs. At lower bias, the energy levels are highly localized with a large energy separation in comparison with QD energy levels at higher V_{DS}. The drain's TB potential decreases, due to the strong electric field, making the QD states less localized, particularly those at very high energies. By increasing the drain bias, higher QD energy levels are pulled down to lower energies. Note that the current spectra presented in the Fig. 3, at first glance, seems similar. However, the two simulations differ by two orders of magnitude. The peaks in the current occur when a single or group of energy levels in the dot enter into resonance with the Fermi-level in the source (E_{FS} = 0 eV). As soon as these levels go below the source subband energy, at x = 0 nm, the current decreases abruptly.

Next, statistical sources of variability were intorduced, such as a RDD. RDD is only considered in the Si parts of

Authorized licensed use limited to: University of Glasgow. Downloaded on June 11,2020 at 10:48:32 UTC from IEEE Xplore. Restrictions apply.

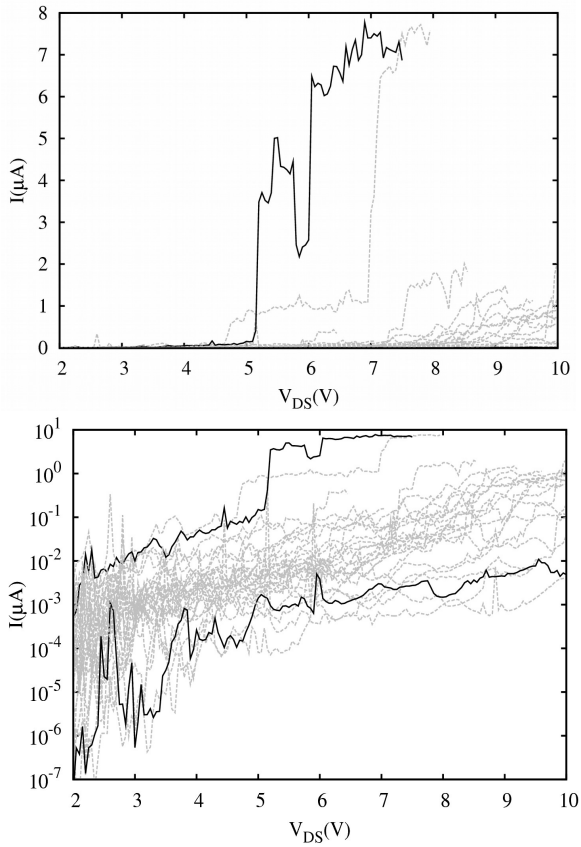

Figure 4. Top (linear scale) and bottom (log scale) of the *I*–*V*DS characteristics of an ensemble of 60 different dot-in-wire devices, each containing a random distribution of dopants (grey curves). The lowest and highest lines, shown in black, are for the RDD configurations shown in Fig. 6.

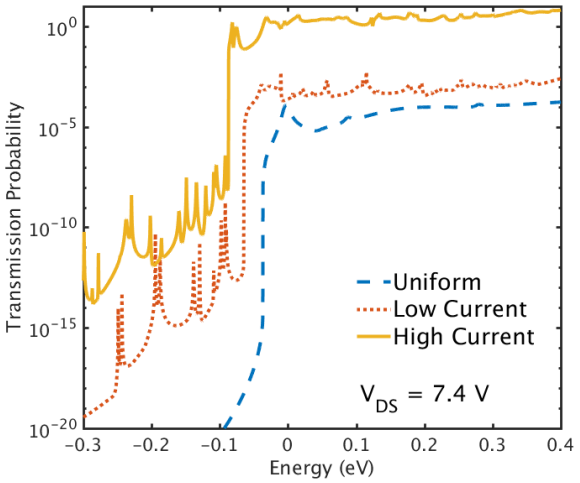

Figure 5. The calculated transmission probability for the 'smooth' device (blue) and both devices with low (red) and high (yellow) current from Fig. 3. The current spectrum is extracted at V_{DS} = 7.4V.

the device. At the source and the drain part of the channel, the RDD region is 5 nm long, preceded by a uniform doped region that is required for numerical stability. The number of dopants in each of the dots is randomly chosen from a Poisson distribution, with the mean determined by the doping concentration multiplied by the volume of the RDD region. The dopants are then randomly placed using a probability rejection technique. For the statistical study presented here, an ensemble of 60 dot-in-wire devices were simulated.

Fig. 4 shows I-V_{DS} curves both on a linear (top) and log (bottom) scale for the ensemble of 60 devices that were simulated. This clearly shows strong variability in the characteristics for each device, which derives only from the RDD. For example, the current at V_{DS}=2V has a distribution of more than 5 orders of magnitude and the same trend is observed at all other V_{DS} values. Each I-V_{DS} curve, in Fig. 4, is unique, being different from one another and is characterized by numerous peaks and valleys. This uniqueness behavior of each dot can be defined, similar to the human fingerprints, as the device fingerprint. In our case, the physical sources of variation is the position and the number of the random dopants in the source, drain and dot regions. The fingerprint from each device can be derived from the complex fluctuations in the tunneling current, which are sensitive to atom-scale variations in the structure.

The current in the device is calculated by using the Landauer-Buttiker formula

$$\mathrm{I}(\mathrm{V}) = \frac{e}{h}\int T(E,V)[f(E-\mu_L) - f(E-\mu_R)]\,dE$$

where e is the charge of electron, h is the Plank's constant, T(E,V) is the transmission and $f(E-\mu_{L(R)})$ is the Fermi-Dirac function for the left and right electrodes with the chemical potential $\mu_{L(R)}$. Hence, the current is directly proportional to the transmission (T), where higher transmission means higher current.

Fig. 5 compares the transmission spectra for the uniform device, the low current and high current devices presented in Fig. 2 and Fig. 4, correspondingly. The transmission current for the 'smooth' device shows the expected stair-type behavior. The low current device shows a similar oscillation of the transmission spectra to those oscillation of the current. The peaks and the values of the transmission spectra can be linked to constructive interference of the electron waves coming from the source to the QD. Also, the positions and the profile of the peaks depend on the positions and the number of the random dopants in the device. Lastly, the T(E) for the higher current device is the highest. This is in agreement with the fact that this device shows the higher current.

The results presented in Fig. 4 can be correlated with the number of dopants and their position in the Si body of the devices. Fig. 6 shows the LDOS, current spectra and the dopant distribution for dot-in-wire devices with low and high current, highlighted in black in Fig. 4, at V_{DS} = 7.5 V. The tunneling current differs between these two devices by around 10^3 times. This large variation significant difference in the I-V_{DS} curves is due to the number and the position of dopants along the whole devices. For instance, the QD with the lower current has 5 dopants in the source and 2 in the QD region. Whereas, the device with the

Authorized licensed use limited to: University of Glasgow. Downloaded on June 11,2020 at 10:48:32 UTC from IEEE Xplore. Restrictions apply.

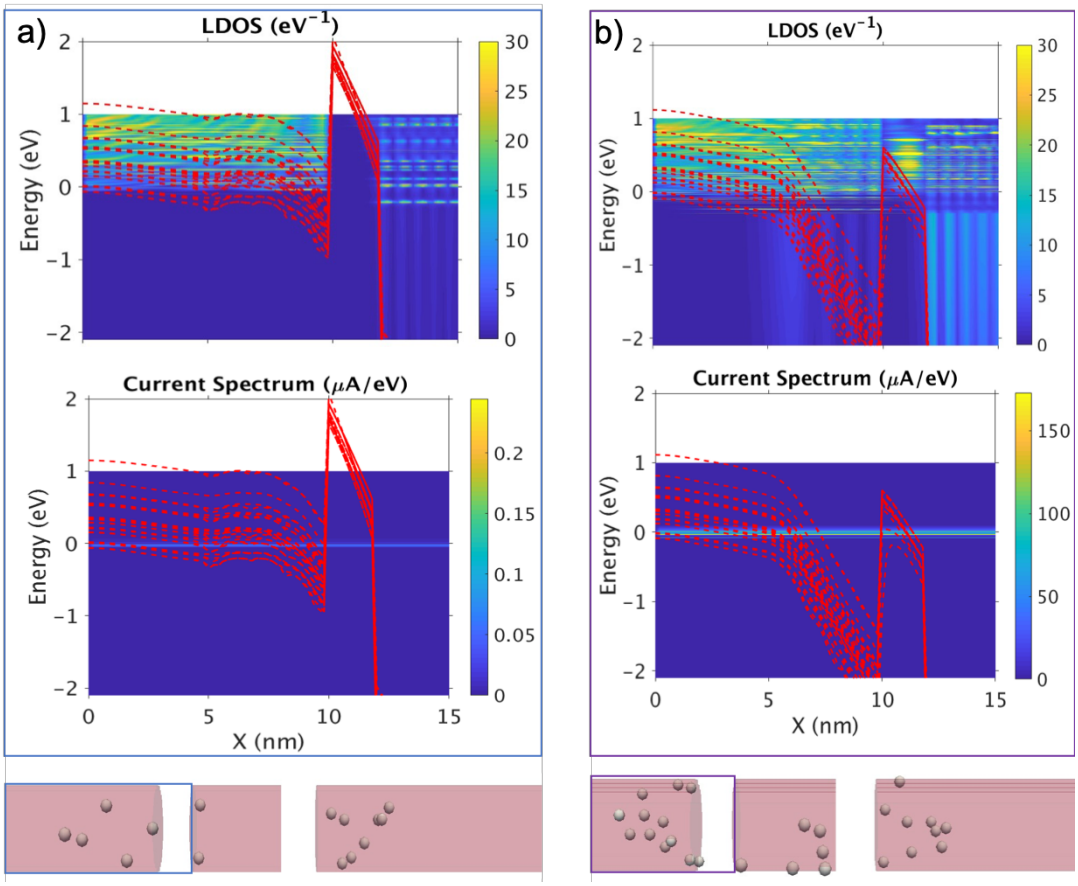

Figure 6. Local density of states (LDOS, top), current spectrum (middle) and dopant distribution (bottom) for a QD with a low current (a) and a high current (b). Only the LDOS and current spectrum around the tunneling barrier close to the source are shown at V_{DS} = 7.5 V. The red lines are the subband profiles and the colored boxes present the device regions, which are plotted for the current spectra and LDOS.

highest current has 12 and 6 in the source and QD regions, respectively. By comparing the subband profiles of the devices, it can be seen that the dopants close to the source/TB interface enhances the electric field in the transport direction. The bigger the number of dopants, the steeper is the potential at the source/TB interface. Consequently, the TB is shorter and thinner in the device with high current. Moreover, the larger number of dopants creates more states in the QD region, acting as available resonant states for the electrons to tunnel through.

In conclusion, in this paper we have reported ballistic quantum mechanical simulations based on the NEGF approach. We simulated an ensemble of 60 devices, each with a different specific random dopant distribution. The simulated dot-in-wire devices each showed a unique I-V_{DS} curve, due to the unique RDD in the entire Si region. Hence, unique I-V_{DS} characteristics can be defined as quantum fingerprints and applied to problems in cybersecurity, such as authentication and identification. Here we have also established a link between the RDD position, the transmission spectra, current spectrum and LDOS. Our work captures the complex nature of the quantum effects in such ultra-small-scaled devices and it can be used for investigating quantum mechanical effects in not only the dot but also in conventional transistors.

REFERENCES

[1] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," *IEEE Access,* vol. 4, pp. 61-80, 2016.

[2] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," *Applied Physics Reviews,* vol. 6, no. 1, pp. 011303, 2019.

[3] I. Papakonstantinou and N. Sklavos, "Physical Unclonable Functions (PUFs) Design Technologies: Advantages and Trade Offs," in *Computer and Network Security Essentials*, 2018, pp. 427-442.

[4] Z. Hu *et al.*, "Physically unclonable cryptographic primitives using self-assembled carbon nanotubes," *Nat Nano,* Article vol. 11, no. 6, pp. 559-565, 06//print 2016.

[5] F. Tehranipoor, N. Karimian, W. Yan, and J. A. Chandy, "DRAM-Based Intrinsic Physically Unclonable Functions for System-Level Security and Authentication," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* vol. 25, no. 3, pp. 1085-1097, 2017.

[6] J. Roberts *et al.*, "Using Quantum Confinement to Uniguely Identify Devices," *Sci Rep*, vol. 5, pp. 16456, 2015.

[7] S. Berrada *et al*., "NESS: New flexible Nano-Electronic Simulation Software," International Conference on Simulation of Semiconductor Processes and Devices (SISPAD), pp. 22-25, 2018

Authorized licensed use limited to: University of Glasgow. Downloaded on June 11,2020 at 10:48:32 UTC from IEEE Xplore. Restrictions apply.